UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,797	02/10/2004	Ramarathnam Venkatesan	MS307073.01/MSFTP588US	9675

27195 7590 02/13/2007

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

BEST AVAILABLE COPY **Office Action Summary**	**Application No.** 10/775,797	**Applicant(s)** VENKATESAN ET AL.	
	Examiner Fatoumata Traore	**Art Unit** 2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *06/01/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response of the original filing of February 10, 2004. Claims 1-35 are pending and have been considered below.

Examiner note

The applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in claim 33 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer programs modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 12 recites the limitation "a sequence" in claim 12. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1- 4, 19, 28, 30, 31, 33-35 are rejected under 35 U.S.C. 102(e) as being anticipated by **Gligor et al** (US 6973187).

Claims 1, 34, 35: **Gligor Et al** discloses a system and computer readable medium comprising:

a. A component that receives a first code (a step of receiving an input plaintext string) (column 6, lines 28-44);

b. And a transformation component that transforms the first code to a new code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary (to create a plurality of hidden cipher text blocks each of 1 bits in length) (column 6, lines 48-52).

Claim 2: **Gligor Et al** discloses a system as in claim 1 above, and further discloses that the new code appears random to the computationally bounded adversary (Performing a randomization function over the plurality of hidden ciphertext blocks to create a plurality of output blocks) (column 6, lines 50-55).

Claim 3: **Gligor Et al** a system as in claim 1 above, and further discloses that the adversarial attack by the bounded adversary on the new code is randomly distributed on the first code (the randomization function step comprises combining each of the hidden ciphertext blocks with a corresponding elements of sequence of unpredictable elements to create a set of output blocks) (column 6, lines 60-70).

Claim 4: **Gligor Et al** discloses a system as in claim 1 above, and further discloses that the transformation component comprises a pseudo-random number generator that facilitates transforming the first code into the new code (the secret random number is provided by a random number generator) (column 7, lines 53-55).

Claim 19: **Gligor et al** discloses a system as in claim 1 above, and **Gligor et al** further discloses that the first code including information relating to authorization of use of the first code, and further comprising a tracing component that determines whether a user is authorized to use the first code (the verifying

integrity step comprises creating an MDC decryption block by applying the non cryptographic Manipulation Detection Code function) (column 9, lines 5-12).

Claim 28: **<u>Gligor Et al</u>** discloses a method comprising:

a. Receiving a message that is desirably transferred to an authorized user code (a step of receiving an input plaintext string) (column 6, lines 28-44);

b. Encoding the message utilizing an encoding scheme designed in a noise model (to create a plurality of hidden cipher text blocks each of 1 bits in length) (column 6, lines 48-52),

c. And algebraically transforming the encoded message into a first code, the first code rendered random to an unauthorized user (to create a plurality of hidden cipher text blocks each of 1 bits in length) (column 6, lines 48-52).

Claim 30: **<u>Gligor Et al</u>** discloses a method as in claim 28 above, and further discloses that the embedding of information into the first code relating to the message's position within a sequence of messages (the assembling step comprises including in the ciphertext string the number of ciphertext segments, a ciphertext segment index, a length of each ciphertext segment and a sequence of ciphertext segments (column 9, lines 60-70).

Claim 31: **<u>Gligor Et al</u>** discloses a method as in claim 28 above, and further discloses that the decoding of the first code is based at least in part upon knowledge of the message's position within a sequence of messages (the step of generating a secret random vector from a secret random number generated on per message basis) (column 7, lines 7-15).

Claim 33: **<u>Gligor Et al</u>** discloses a system comprising:

a. Means for receiving a first code (a step of receiving an input plaintext string) (column 6, lines 28-44);

b. Means for transforming the first code into a second code, the second code appearing random to a computationally bounded adversary and having substantially similar length as the first code (to create a plurality of hidden cipher text blocks each of 1 bits in length) (column 6 lines 48-52);

c. And means for decoding the second code to obtain the first code (a decryption program is provided) (column 11, lines 50-70).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Gligor et al** (US 6973187).

Claim 32: **Gligor Et al** discloses a method as in claim 31 above, and further discloses generating a seed (the step of generating the secret random number by enciphering a count of counter initialized to a constant, the enciphering being performed with the block cipher using the secret first key; and incrementing the counter by one on every message encryption) (column 7, lines 55-62); generating random numbers a and b based at least in part upon the seed (the step of generating a secret random vector from a secret random number generated on per message basis) (column 7, lines 7-15), wherein a and b have a length of n bits partitioning the input plaintext string into a plurality of equal size blocks) (column 6, lines 39-55); embedding the seed into the first code(generating the secret random number by enciphering a count of counter initialized to a constant (seed) (column 7, lines 55-60), but **Gligor et al** does not disclose generating a random permutation. sigma. that permutes the n bits. However, **Gligor et al** discloses a step of generating the secret random vector by generating a modular 2.sup.I multiplication and addition (column 8, lines 20-35). Additionally, since the generated permutation is not used in the claim, little, if any patentable weight is given to how it was generated. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was

made to include a random permutation sigma that permutes the n bits. One would have been motivated to do so in order to increase system security.

3. Claims 5-8, 11-18, 20–23, 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gligor et al** (US 6973187) in view of **Bohnke** (US 6557139).

Claim 5: **Gligor Et al** discloses a system as in claim 1 above, but does not explicitly disclose that the system has a decoder. However, **Bohnke** discloses a similar system that further discloses a decoder (figure 4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include a decoder. One would have been motivated to retrieve the plain-text file (first code) at the receiving end.

Claim 6: **Gligor et al** and **Bohnke** disclose a system as in claim 5 above, and **Bohnke** further discloses that the decoder comprises a checking component that determines whether the first code has been corrupted (the decoding iteration means only performs one iteration at a time and is controlled or triggered by a control signal from the checking means to continue the decoding processing in case that the checking result indicates that the decode information are not yet correct) (column 4, lines 55-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al**

to include a checking component. One would have been motivated to do so in order ensure processing with non-corrupted code.

Claim 7: **Gligor et al** and **Bohnke** disclose a system as in claim 6 above, and **Bohnke** further discloses that the checking component utilizing a checking function h:.SIGMA..sup.n>[0,1], where .SIGMA. is a finite alphabet that defines a family of codes and n is a length parameter for .SIGMA (The means for checking the decoded information is a cyclic redundancy checksum checking means in the example shown in FIG. 4, which detects errors in the transmitted data d.sub.0, d.sub.1, . . . , d.sub.N-1 on the basis of the appended checksum bits C.sub.0, . . . , C.sub.M-1 of each frame. The hard decision means transforms the soft decision values output from the turbo decoder into hard decision values, e. g. bits ("0" or "1") (column 6, lines 45-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include a checksum means in the decoder. One would have been motivated to do so in order to ensure that the transmitted data was properly received.

Claim 8: **Gligor et al** and **Bohnke** disclose a system as in claim 6 above, and **Bohnke** further discloses that the checking component outputting a vector, the first code being corrupted when the vector is a non-zero vector (The checking means performs a cyclic redundancy check to detect errors in the transmitted

data. If an error is detected in the transmitted data d.sub.0, d.sub.1, . . . d.sub.N-1, a control signal is generated and fed back to the turbo decoder (column 6, lines 60-65). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include outputting an indication of corrupted data. One would have been motivated to do so in order to alert the user when the transmitted data was not properly received.

Claim 11: **Gligor et al** and **Bohnke** disclose a system as in claim 5 above, and **Gligor et al** further discloses that the first code is generated based at least in part on a sequence of messages (the assembling step comprises including in the ciphertext string the number of ciphertext segments, a ciphertext segment index, a length of each ciphertext segment and a sequence of ciphertext segments (column 9, lines 60-70).

Claim 12: **Gligor et al** and **Bohnke** disclose a system as in claim 11 above, and **Gligor et al** further discloses that the decoder knowing a sequence of messages (decrypting each ciphertext segment using the different secret random number by ciphertext segment to obtain a plain text segment using the decryption method) (column 10, lines 33-35).

Claim 13: **Gligor et al** and **Bohnke** disclose a system as in claim 12 above, and **Gligor et al** further discloses that the pseudo random number generator

generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages (the step of generating a secret random vector from a secret random number generated on per message basis) (column 7, lines 7-15), but does not explicitly disclose that the pseudo random number generator further generates a random permutation .sigma, that permutes the n bits. However, **Gligor et al** discloses a step of generating the secret random vector by generating a modular 2.sup.l multiplication and addition (column 8, lines 20-35). Additionally, since the generated permutation is not used in the claim, little, if any patentable weight is given to how it was generated. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was me to include a random permutation sigma that permutes the n bits. One would have been motivated to do so in order to increase system security.

Claim 14: **Gligor et al** and **Bohnke** disclose a system as in claim 11 above, and **Gligor et al** further discloses that the transformation component sends a randomized code word to the decoder, the randomized code word having the form a.times..sigma.(f(m.sub.i))+b, where f is an encoding function, m is a message, i is the position of the message within the sequence, and x is a bitwise multiplication operator(the steps of: presenting a string including ciphertext string for decryption; partitioning the ciphertext string into a plurality of ciphertext blocks comprising l bits each; selecting n+1 ciphertext blocks from the plurality of

ciphertext blocks representing n data blocks and one MDC block and performing a reverse randomization function on each of the selected n+1 ciphertext blocks to obtain a plurality of hidden ciphertext blocks)(column 8, lines35-45) .

Claim 15: **Gligor et al** and **Bohnke** disclose a system as in claim 11 above, and **Gligor et al** further discloses that the transformation component embeds information relating to the sequence of messages into the new code (the step of generating the secret random number by enciphering a count of counter initialized to a constant, the enciphering being performed with the block cipher using the secret first key; and incrementing the counter by one on every message encryption) (column 7, lines 55-62).

Claim 16: **Gligor et al** and **Bohnke** disclose a system as in claim 15 above, and **Gligor et al** further discloses that the first code has a length of n.sub.l, and the information relating to the sequence of messages embedded in n.sub.l locations in the new code(to create a plurality of hidden ciphertext blocks each of one 1 bits in length and performing a randomization function over the plurality of hidden blocks to create a plurality of output ciphertext block each of each of 1 bits in length(column 6, lines 48-55).

Claim 17: **Gligor et al** and **Bohnke** disclose a system as in claim 16 above, and **Gligor et al** further discloses that the pseudo random number generator

generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages (the step of generating a secret random vector from a secret random number generated on per message basis) (column 7, lines 7-15), but does not explicitly disclose that the pseudo random number generator further generates a random permutation sigma, that permutes the n bits. However, **Gligor et al** discloses a step of generating the secret random vector by generating a modular 2.sup.l multiplication and addition (column 8, lines 20-35). Additionally, since the generated permutation is not used in the claim, little, if any patentable weight is given to how it was generated. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was me to include a random permutation sigma that permutes the n bits. One would have been motivated to do so in order to increase system security.

Claim 18: **Gligor et al** and **Bohnke** disclose a system as in claim 17 above, and **Gligor et al** further discloses that an encoder sending the new code to the decoder, the new code having embedded therein the seed (generating the secret random number by enciphering a count of counter initialized to a constant (seed) (column 7, lines 55-60).

Claim 20: **Gligor Et al** discloses a system comprising:

A code generator that generates a first code based at least in part upon a sequence of messages that are desirably relayed to a receiver (the step of receiving an input plain text string, partitioning the input plaintext string into a plurality of equal size blocks, creating a Manipulation Detection Code to the plurality of equal sizes blocks, making one pass to create a plurality of hidden ciphertext) (column 6, lines 39-55);

A code hiding module that creates a second code, the second code being a pseudo random version of the first code, the second code appears to be random to a computationally bounded adversary (to create a plurality of hidden ciphertext blocks each of 1 bits in length; and performing a randomization function over the plurality of hidden ciphertext blocks each of 1 bits in length) (column 6, lines 49-55); but do not explicitly disclose a decoder that determines the first code from the second code. However, **Bohnke** discloses a decoder (figure 4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a decoder. One would have been motivated to do so in order to retrieve the plaint-text file (first code) at the receiving end.

Claim 21: **Gligor et al** and **Bohnke** disclose a system as in claim 20 above, and **Bohnke** further discloses an encoding component that encodes a message and creates a code word, the encoding component encodes the message with a code that has a minimum relative distance. epsilon. and rate 1-.kappa..epsilon. for some constant .kappa.>1. (In FIG. 3, a block diagram of an encoding structure

according to the present invention is shown, which comprises a data input means, a checksum generator, a frame formatter and a turbo encoder. The data input means receives serially arranged data bits, e. g. in data frames consisting of N data bits, d.sub.0, d.sub.1, . . . d.sub.N-1. (Column 5, lines 50-55). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include such an encoder. One would have been motivated to do so in order to increase data and system security.

Claim 22: **Gligor et al** and **Bohnke** disclose a system as in claim 21 above, and **Gligor et al** further discloses a component that utilizes the encoded message and divides the encoded message into a number of blocks B, the B blocks being of substantially similar size (the step of receiving an input plaintext string comprising a message and padding it as necessary such that its length is a multiple of 1 bits; partitioning the input plaintext string a length that is a multiple of one bits in to a plurality of equal size blocks (column 6, lines 38-45).

Claim 23: **Gligor et al** and **Bohnke** disclose a system as in claim 20 above, and **Bohnke** further discloses that the plurality of blocks encoded using (n, k, n-k+1) Reed-Solomon code (In this case, an error correction code, e. g. a BCH codec to detect and correct bit errors or an RS (Reed-Solomon) codec to detect and correct symbol errors is generated and added to the data to be transmitted in the

encoding apparatus of the present invention) (column 7, lines 25-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to use Reed_Solomon code. One would have been motivated to do so in order to increase data integrity and system security.

Claim 29: **Gligor Et al** discloses a method as in claim 28 above, but does not explicitly disclose that the message is decoded at least in part by solving a minimum vertex cover problem. However, **Bohnke** discloses a similar system that further discloses that the message is decoded at least in part by solving a minimum vertex cover problem (the decoding iteration means only performs one iteration at a time and is controlled or triggered by a control signal from the checking means to continue the decoding processing in case that the checking result indicates that the decoded information are not yet correct) (column 4, lines 55-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to use such decoding processing. One would have been motivated to so in order to increase data security.

4. Claims 9, 10, 24, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gligor et al** (US 6973187) in view of **Bohnke** (US 6557139),

in further view of **Guruswami** (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages: 658- 667, ISBN: 0-7695-1116-3).

Claim 9: **Gligor et al** and **Bohnke** disclose a system as in claim 5 above. While neither reference explicitly discloses that the decoder utilizes a unique decoding function, **Guruswami** discloses a similar system, which further discloses a decoder utilizing a unique decoding function (we further consider the list decoding version) (introduction and section 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include such a unique decoding function. One would have been motivated to do so in order to increase data integrity and system security.

Claim 10: **Gligor et al** and **Bohnke** disclose a system as in claim 5 above. While neither reference explicitly discloses that the decoder utilizes a list decoding function g, **Guruswami** discloses a similar system, which further discloses a decoder utilizing a list decoding function (we further consider the list decoding version) (introduction and section 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include a list decoding function. One would have been motivated to do so in order to increase data and system security.

Claim 24: **Gligor et al** and **Bohnke** disclose a system as in claim 23 above. While neither reference explicitly discloses that the code hiding module comprising a bipartite expander graph with a number of edges being substantially similar to Bn, and symbols within the B blocks are randomly assigned an edge within the bipartite expander graph, **Guruswami** discloses a similar system, which further discloses an expander graph with a number of edges being substantially similar to Bn, and symbols within the B blocks are randomly assigned an edge within the bipartite expander graph(the construction employ expander graphs, which facilitate efficient decoding algorithms through various forms of voting procedures) (introduction and section 4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include a list decoding function. One would have been motivated to do so in order to increase data and system security.

Claim 25: **Gligor et al** and **Bohnke** disclose a system as in claim 20 above. While neither reference explicitly discloses that the decoder comprises one or more algorithms that facilitate solving a minimum vertex cover problem, **Guruswami** discloses a similar system, which further discloses the decoder comprises one or more algorithms that facilitate solving a minimum vertex cover problem (the construction employ expander graphs, which facilitate efficient decoding algorithms through various forms of voting procedures and further consider both unique and list decoding versions) (introduction). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include various decoding algorithms. One would have been motivated to do so in order to increase system portability.

5. Claims 26, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gligor et al** (US 6973187) in view of **Bohnke** (US 6557139), in further view of **Lee et al** (US 6792542).

Claim 26: **Gligor et al** and **Bohnke** disclose a system as in claim 20 above. While neither reference explicitly discloses a synchronization component that synchronizes the code generator with the decoder, **Lee et al** discloses a similar system, which further discloses a synchronization component (figure 7 and 8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to include a synchronization component. One would have been motivated to do so in order to maintain system integrity.

Claim 27: **Gligor et al** and **Bohnke** disclose a system and as in claim 20 above. While neither reference explicitly discloses that the code-hiding module embeds synchronization information into the second code, **Lee et al** discloses a similar system, which further discloses a synchronization component embedding information into the code (figure 7 and 8). Therefore, it would have been obvious

to one having ordinary skill in the art at the time the invention was made for **Gligor et al** to embed such data into the code. One would have been motivated to do so in order to make the information available to the receiver/decoder.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Chung et al (US 4779266) encoding and decoding for code division multiple access communication system.
- Laih et al (US 6144740) Method for designing public cryptosystem against fault based attacks with an implementation.
- Aminetzah (US 4388643) Method of controlling scrambling and unscrambling in pay TV system.
- Hekstra (US 6543025) Transmission system with adaptive channel encoder and decoder.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number

for Formal or Official faxes to Technology Center 2100 is (571) 273-3800. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
February 7, 2007

James W. Myhre
Supervisory Patent Examiner